Exhibit B

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

WIDEVINE TECHNOLOGIES, INC.	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. 2-07-cv-321
	§	
VERIMATRIX, INC.,	§	
Defendant.	§	
	§	
	§	
	§	

MEMORANDUM OPINION AND ORDER

After considering the submissions and the arguments of counsel, the Court issues the following order concerning the claim construction issues:

I. Introduction

Widevine Technologies, Inc. (“Widevine”) asserts United States Patent Nos. 7,165,175 (“the ‘175 patent”) and 7,376,831 (“the ‘831 patent”) against Verimatrix, Inc. (“Verimatrix”). Widevine and Verimatrix both provide encryption technology that protects digital media content. Widevine explains that its technology is used by telecommunications providers to protect premium television content as it is distributed across digital networks to customers’ homes. Verimatrix describes its technology as applications that protect video and audio content during the distribution process to prevent the unauthorized consumption or distribution of content.

II. Background of the Technology

The ‘175 patent has a priority date of September 6, 2000 and issued January 16, 2007. The ‘831 patent is a continuation of the ‘175 patent, filed on August 25, 2006 and issued on May 20, 2008. Both patents teach a system and method for parsing, selectively encrypting, and decrypting different portions of data during transmission from a server (such as the cable company) to the client (such as the TV set top box). The inventions teach performing the parsing, encryption, and decryption in real-time. The data is transmitted over the network in packets. A multimedia file, for example, will be composed of many packets during transmission.

The patents disclose an “encryption bridge” that performs the selective encryption of the packets. The encryption bridge is the software that operates between the multimedia server, for example, and the network. During distribution of data from the server to the network, the encryption bridge examines each of the packets to determine whether a packet needs to be encrypted and, if so, what part of the packet needs to be encrypted. The specification explains that this enables the proprietary data (i.e., a copyrighted multimedia file) to be encrypted without having to encrypt the portion of a packet that contains routing information. According to the claims and the specification, the encryption bridge examines at the packet to determine whether the payload portion of a packet matches a predefined data type. The specification offers the Windows Media format as an example of a predefined data type. If the data matches the predefined data type, the encryption bridge will encrypt the proprietary data in the payload, leaving the non-proprietary data untouched.

The patents also disclose a “shim” that receives the packets over the network from the encryption bridge. The shim is software that is installed on a client, such as a computer, multimedia player, or cable box. The shim decrypts the packets at the client, making the proprietary data available for the client customer.

The encryption protects the proprietary information from unauthorized copying during distribution from the server to the client. In a packet-switching network, such as the Internet, a data packet travels along a path between routers that are owned and maintained by third-parties. Two packets that are part of the same transmission might not follow the same route between a server and a client. During transmission, when a packet arrives at an intermediate router, that router determines the best subsequent path to the packet's given destination. Changed conditions might cause the same router to send two related packets on two different paths. To take full advantage of a packet-switched network, the routing information must be visible by all intermediate routers. This allows the greatest possible number of paths from the server to the client, which will guarantee the fastest available transmission. If the routing information is encrypted, the packet's transmission is limited to predetermined paths, which might result in a slower transmission than would otherwise be available. The invention protects the proprietary data while leaving the routing information unencrypted so that the distribution from the server to the client takes the fastest possible route.

III. General Principles Governing Claim Construction

"A claim in a patent provides the metes and bounds of the right which the patent confers on the patentee to exclude others from making, using or selling the protected invention." *Burke, Inc. v. Bruno Indep. Living Aids, Inc.*, 183 F.3d 1334, 1340 (Fed. Cir. 1999). Claim construction is an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996).

To ascertain the meaning of claims, the court looks to three primary sources: the claims, the specification, and the prosecution history. *Markman*, 52 F.3d at 979. Under the patent law, the specification must contain a written description of the invention that enables one of ordinary skill in the art to make and use the invention. A patent's claims must be read in view of the specification, of which they are a part. *Id*. For claim construction purposes, the description may act as a sort of dictionary, which explains the invention and may define terms used in the claims. *Id*. "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." *Watts v. XL Sys., Inc.*, 232 F.3d 877, 882 (Fed. Cir. 2000).

Nonetheless, it is the function of the claims, not the specification, to set forth the limits of the patentee's claims. Otherwise, there would be no need for claims. *SRI Int'l v. Matsushita Elec. Corp*., 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). The patentee is free to be his own lexicographer, but any special definition given to a word must be clearly set forth in the specification. *Intellicall, Inc. v. Phonometrics*, 952 F.2d 1384, 1388 (Fed. Cir. 1992). And, although the specification may indicate that certain embodiments are preferred, particular embodiments appearing in the specification will not be read into the claims when the claim language is broader than the embodiments. *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994).

This court's claim construction decision must be informed by the Federal Circuit's decision in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). In *Phillips*, the court set forth several guideposts that courts should follow when construing claims. In particular, the court reiterated that "the *claims* of a patent define the invention to which the patentee is entitled the right to exclude." 415 F.3d at 1312 (emphasis added) (*quoting Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To that end, the words used in a claim are generally given their ordinary and customary meaning. *Id*. The ordinary and customary meaning of a claim term "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id*. at 1313. This principle of patent law flows naturally from the recognition that inventors are usually persons who are skilled in the field of the invention. The patent is addressed to and intended to be read by others skilled in the particular art. *Id*.

The primacy of claim terms notwithstanding, *Phillips* made clear that "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id*. Although the claims themselves may provide guidance as to the meaning of particular terms, those terms are part of "a fully integrated written instrument." *Id*. at 1315 (*quoting Markman*, 52 F.3d at 978). Thus, the *Phillips* court emphasized the specification as being the primary basis for construing the claims. *Id*. at 1314-17. As the Supreme Court stated long ago, "in case of doubt or ambiguity it is proper in all cases to refer back to the descriptive portions of the specification to aid in solving the doubt or in ascertaining the true intent and meaning of the language employed in the claims." *Bates v. Coe*, 98 U.S. 31, 38 (1878). In addressing the role of the specification, the *Phillips* court quoted with approval its earlier observations from *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998):

> Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction.

Consequently, *Phillips* emphasized the important role the specification plays in the claim construction process.

The prosecution history also continues to play an important role in claim interpretation. The prosecution history helps to demonstrate how the inventor and the PTO understood the patent. *Phillips*, 415 F.3d at 1317. Because the file history, however, "represents an ongoing negotiation between the PTO and the applicant," it may lack the clarity of the specification and thus be less useful in claim construction proceedings. *Id*. Nevertheless, the prosecution history is intrinsic evidence. That evidence is relevant to the determination of how the inventor understood the invention and whether the inventor limited the invention during prosecution by narrowing the scope of the claims.

Phillips rejected any claim construction approach that sacrificed the intrinsic record in favor of extrinsic evidence, such as dictionary definitions or expert testimony. The *en banc* court condemned the suggestion made by *Texas Digital Systems, Inc. v. Telegenix, Inc.*, 308 F.3d 1193 (Fed. Cir. 2002), that a court should discern the ordinary meaning of the claim terms (through dictionaries or otherwise) before resorting to the specification for certain limited purposes. *Id*. at 1319-24. The approach suggested by *Texas Digital*–the assignment of a limited role to the specification–was rejected as inconsistent with decisions holding the specification to be the best guide to the meaning of a disputed term. *Id*. at 1320-21. According to *Phillips*, reliance on dictionary definitions at the expense of the specification had the effect of "focus[ing] the inquiry on the abstract meaning of words rather than on the meaning of the claim terms within the context of the patent." *Id*. at 1321. *Phillips* emphasized that the patent system is based on the proposition that the claims cover only the invented subject matter. *Id*. What is described in the claims flows from the statutory requirement imposed on the patentee to describe and particularly claim what he or she has invented. *Id*. The definitions found in dictionaries, however, often flow from the editors' objective of assembling all of the possible definitions for a word. *Id*. at 1321-22.

Phillips does not preclude all uses of dictionaries in claim construction proceedings. Instead, the court assigned dictionaries a role subordinate to the intrinsic record. In doing so, the court emphasized that claim construction issues are not resolved by any magic formula. The court did not impose any particular sequence of steps for a court to follow when it considers disputed claim language. *Id*. at 1323-25. Rather, *Phillips* held that a court must attach the appropriate weight to the intrinsic sources offered in support of a proposed claim construction, bearing in mind the general rule that the claims measure the scope of the patent grant.

The patents-in-suit include claim limitations that fall within the scope of 35 U.S.C. § 112 ¶ 6. "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure. . . in support thereof, and such claim shall be construed to cover the corresponding structure . . . described in the specification and equivalents thereof." 35 U.S.C. § 112 ¶ 6. When a claim uses the term "means" to describe a limitation, a presumption inheres that the inventor used the term to invoke § 112 ¶ 6. *Biomedino, LLC v. Waters Techs. Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007). "This presumption can be rebutted when the claim, in addition to the functional language, recites structure sufficient to perform the claimed function in its entirety." *Id.* (citing *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1375 (Fed. Cir. 2003)). Once the court has concluded the claim limitation is a means-plus-function limitation, the first step in construing a means-plus-function limitation is to identify the recited function. *See Micro Chem., Inc. v. Great Plains Chem. Co.*, 194 F.3d 1250, 1258 (Fed. Cir. 1999). The second step in the analysis is to identify in the specification the structure corresponding to the recited function. *Id.* The "structure disclosed in the specification is 'corresponding' structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim." *Medical Instrumentation and Diagnostics Corp. v. Elekta AB*, 344 F.3d 1205, 1210 (Fed. Cir. 2003), *citing B. Braun v. Abbott Labs*, 124 F.3d 1419, 1424 (Fed. Cir. 1997).

The patentee must clearly link or associate structure with the claimed function as part of the quid pro quo for allowing the patentee to express the claim in terms of function pursuant to

§ 112 ¶ 6. *See id.* at 1211; *see also Budde v. Harley-Davidson, Inc.*, 250 F.3d 1369, 1377 (Fed. Cir. 2001). The "price that must be paid" for use of means-plus-function claim language is the limitation of the claim to the means specified in the written description and equivalents thereof. *See O.I. Corp. v. Tekmar Co.*, 115 F.3d 1576, 1583 (Fed. Cir. 1997). "If the specification does not contain an adequate disclosure of the structure that corresponds to the claimed function, the patentee will have 'failed to particularly point out and distinctly claim the invention as required by the second paragraph of section 112,' which renders the claim invalid for indefiniteness." *Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1382 (Fed. Cir. 2009), *quoting In re Donaldson Co.*, 16 F.3d 1189, 1195 (Fed. Cir. 1994) (en banc). It is important to determine whether one of skill in the art would understand the specification itself to disclose the structure, not simply whether that person would be capable of implementing the structure. *See Atmel Corp. v. Info. Storage Devices, Inc.*, 198 F.3d 1374, 1382 (Fed. Cir. 1999); *Biomedino*, 490 F.3d at 953. Fundamentally, it is improper to look to the knowledge of one skilled in the art separate and apart from the disclosure of the patent. *See Medical Instrumentation*, 344 F.3d at 1211-12. "[A] challenge to a claim containing a means-plus-function limitation as lacking structural support requires a finding, by clear and convincing evidence, that the specification lacks disclosure of structure sufficient to be understood by one skilled in the art as being adequate to perform the recited function." *Budde*, 250 F.3d at 1376-77.

At issue in this case is whether certain claims of the patents-in-suit are indefinite. A claim is invalid for indefiniteness if it fails to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. 35 U.S.C. § 112, ¶ 2. To prevail on an indefiniteness argument, the party seeking to invalidate a claim must prove "by clear and convincing evidence that a skilled artisan could not discern the boundaries of the claim based on the claim language, the specification, and the prosecution history, as well as her knowledge of the relevant art area." *Halliburton Energy Servs., Inc. v. M-I LLC*, 514 F.3d 1244, 1249-50 (Fed. Cir. 2008). The primary purpose of the definiteness requirement is to ensure public notice of the scope of the patentee's legal right to exclude, such that interested members of the public can determine whether or not they infringe. *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1347 (Fed. Cir. 2005); *Halliburton*, 514 F.3d at 1249; *Honeywell Int'l Inc. v. Int'l Trade Comm'n*, 341 F.3d 1332, 1338 (Fed. Cir. 2003). Courts apply the general principles of claim construction in their efforts to construe allegedly indefinite claim terms. *Datamize*, 417 F.3d at 1348; *Young v. Lumenis, Inc.*, 492 F.3d 1336, 1346 (Fed. Cir. 2007). A claim is indefinite only when a person of ordinary skill in the art is unable to understand the bounds of the claim when read in light of the specification. *Miles Labs., Inc. v. Shandon, Inc.*, 997 F.2d 870, 875 (Fed. Cir. 1993); *Star Scientific, Inc. v. R.J. Reynolds Tobacco Co.*, 537 F.3d 1357, 1371 (Fed. Cir. 2008). A determination of claim indefiniteness is a conclusion of law. *Exxon Research & Eng'g Co. v. United States*, 265 F.3d 1371, 1375-76 (Fed. Cir. 2001); *Datamize*, 417 F.3d at 1347.

A claim is indefinite only if the claim is "insolubly ambiguous" or "not amenable to construction." *Exxon*, 265 F.3d at 1375; *Young*, 492 F.3d at 1346; *Halliburton*, 514 F.3d at 1249; *Honeywell*, 341 F.3d at 1338-39. A court may find a claim indefinite "only if reasonable efforts at claim construction prove futile." *Datamize*, 417 F.3d at 1347. A claim term is not indefinite solely because the term presents a difficult claim construction issue. *Id.*; *Exxon*, 265 F.3d at 1375; *Honeywell*, 341 F.3d at 1338. "If the meaning of the claim is discernable, even though the task may be formidable and the conclusion may be one over which reasonable persons will disagree, . . . the claim [is] sufficiently clear to avoid invalidity on indefiniteness grounds." *Exxon*, 265 F.3d at 1375; *Halliburton*, 514 F.3d at 1249.

IV. Agreed Constructions

Term	Agreed Construction
Routing information	Bits indicating the destination (i.e., the address of receiving client or the interface or position in a multimedia stream) of the packet data.
Parser	Software on a computing device that analyzes input data to differentiate between different portions of data.
Encrypter	Software on a computing device that encrypts data using an encryption algorithm.
Transparent to the server	Occurring seamlessly on another device, without user interaction on the server.
Transparent to the client	Occurring seamlessly on the shim, without user interaction on the client.
[Passing decrypted data] to a higher level of operations **[Sending decrypted data] to a higher level operation resident on the client**	Passing or sending the decrypted data from the shim to a software application on the client, such as a media player application.
Decrypter	Software in the shim that decrypts data using an encryption or decryption algorithm.
Client	A networked computing device that receives data over a network from a server.
Encrypting	Transforming data using an encryption algorithm and an encryption key into a form that is unreadable or unusable without an encryption or decryption key.
Server	A networked computer device that sends data over a network to one or more clients.
Key **Encryption key** **Decryption key**	A secret code used to encrypt or decrypt information.
Negotiating an encryption key	Two-way communicating between two computing devices to exchange an encryption key in secret over a network.
The client is compromised	The client has been hacked or modified in an unauthorized manner.
Decrypting	Restoring the original unencrypted data using an encryption algorithm and an encryption key or decryption key.
Accepting a shim	Installing a shim.
Volatile memory	Computer memory that requires power to maintain the stored information.
Network	A packet-switched network, such as a network that transmits data using Internet Protocol standards.
Streaming data [noun]	Multimedia data that is being transmitted in real-time.

Term	Agreed Construction
A stream **A data stream** **data stream of packets**	A transmission of multimedia data across a network in real time from a data source to a client.
Streaming session	A period of time in which a media player application on the client is receiving and playing back a particular stream of multimedia data.
A media player resident on the client	A software application on the client that plays multimedia data.
A self-generated certificate	An electronic security certificate generated by the client.
Authenticating a client	Verifying whether the client is authorized to receive and decrypt data.
recognize a predefined data type **recognizing a predefined data type**	Identifying whether the examined payload portion contains the predefined data type.
Encryption bridge	One or more standalone networked encryption devices that receive data from a server over a network, selectively encrypt that data in real time, and transmit that selectively-encrypted data over a network to one or more clients in real time.
Downloading	Transferring data across a network from one network device to another network device.
Streaming [verb] **The streaming of the packets** **Streaming of network packets**	Sending multimedia data in real time over a network.
the payload and non-payload portions	The payload and non-payload portions of the received packet.
Determining a plurality of portions in a packet that includes a payload portion and non-payload portion	Identifying at least two data portions in a packet, including a payload portion and non-payload portion

V. Terms in Dispute

A. "packet," "payload," and "non-payload"

Term	Widevine Proposal	Verimatrix Proposal
Packet	A block of data used for transmitting information that includes at least a header and a payload.	A block of data used for transmitting information.
Payload	The data of interest contained inside of the packet.	just the data of interest.
Non-payload	The packet data that is not payload data, such as header fields and control fields that contain routing or configuration information.	The packet data that is not payload data, including routing or configuration information.

Both parties agree that a "packet" is a "block of data used for transmitting information." The parties dispute whether a packet must also include a header and a payload. The specification explains that, "Data packets can be typically divided into two parts, the header and the payload parts." '175 patent, 4:41–42.

Widevine argues that a packet, according to its plain meaning in the art, must include a header and a payload. Widevine points out that the specification identifies six types of packets, each of which include a header and a payload.

Verimatrix argues that nothing in the intrinsic record requires that a packet have a header and a payload. Verimatrix indentifies a number of telecommunications packets that do not require a payload. Verimatrix also points out that including the word "header" in the definition of a packet will make some terms superfluous in certain unasserted claims. For example, claim 3 of the '175 patent teaches that "the non-payload portion of the packet data includes at least one of a header, control data and routing data." According to Verimatrix, defining "packet" to necessarily include a header would make '175 patent, claim 3 meaningless.

Widevine further argues that, in the context of the claims, a packet must have both a header and a payload. Each of the claims recites performing some action on the "payload portion" of a packet. For example, the '831 patent, Claims 1, 9, and 16 recite "examining a payload portion of the packet." Limitations in the '175 patent, Claims 1, 19, and 37 recite parsing a packet into payload and non-payload portions of a packet. A limitation in the '175 patent, Claim 50 recites, "examining the data of each received packet to identify a plurality of portions that include at least a payload portion and a non-payload portion."

There is not an ordinary meaning for "packet" at the level of detail requested by Widevine in its proposal. The protocol or communications platform determines the composition of a packet. Additionally, some TCP/IP packets (included as an example in the specification in the '175 patent, 2:43–58) are intentionally empty, even though a TCP/IP packet is defined with space for a payload. While *most* packets include a header and a payload, the specification and the claims do not expressly preclude packets without headers or payloads. Even though each claim recites parsing into a payload and non-payload portion, the claims do not preclude non-payload-bearing TCP/IP packets, for example. The invention is capable of ignoring non-payload-bearing packets. Some claims expressly specify that a parsed packet includes both payload and non-payload portions. '175 patent, Claim 19, 37, 50, 58, 64, 74, 81, and 92. Some claims implicitly require multiple portions in a packet, one of which is a payload. *See* '831 patent, claim 1 ("receiving a packet; examining a payload portion of the packet"). Claim 3 of the '175 patent expressly recites that the non-payload portion "includes at least one of a header, control data, and routing data." Construing "packet" to always include a header makes the term "header" in Claim 3 superfluous. Each packet does, however, have a payload portion and non-payload portion. The court construes "packet" to mean "a block of data used for transmitting information that may include payload and non-payload portions."

Both parties agree that "payload" is "data of interest." They dispute whether the definition should require that payload be "contained inside of the packet. Verimatrix draws its proposed construction from the specification, which states, "The payload is the portion of the data packet that is just the data of interest, in exemplary case: multimedia content." '175 patent, 4:44–46. It is the Court's view that the patentee was acting as its own lexicographer when he described a payload as, "the portion of the data packet that is just the data of interest." *See Sinorgchem, Co., Shandong v. Int'l Trade Comm'n*, 511 F.3d 1132, 1138 (Fed. Cir. 2007) ("We have frequently found that a definition set forth in the specification governs the meaning of the claims."). Therefore, the Court's construction of "payload" is "the portion of the data packet that is just the data of interest."

The dispute over "non-payload" is whether it is appropriate to include "header fields" and "control fields" in the construction. Verimatrix argues that Widevine is attempting to import unnecessary terms from the specification. Widevine, on the other hand, argues that Verimatrix's definition is "coextensive" with a header, which inappropriately limits "non-payload" to header data exclusively. The Court agrees that "header fields" and "control fields" do not belong in the definition. The Court is not persuaded, however, that Verimatrix's proposal is so narrow as to exclude any data within a payload that is not in the header. Both "such as" and "including" are permissive words that do not indicate any restriction against the presence of other data in the non-payload portion. Nonetheless, the Court will modify Verimatrix's proposed construction to incorporate Widevine's word choice: "the packet data that is not payload data, such as routing or configuration information."

B. "parsing"

Term	**Widevine Construction**	**Verimatrix Construction**
Parsing	Analyzing data to differentiate between different portions of data.	parse = separate; parsing = separating

The parties agree that a "parser" is "software on a computing device that analyzes input data to differentiate between different portions of data." Widevine proposes a construction that is based upon this agreed definition for "parser." Verimatrix proposes "separating," arguing that the claims and specification show that parsing means separating. The specification explains the benefits of the invention over the prior art:

> Without accurately parsing the data into payload and non-payload parts, the user specific data is readily damaged or scrambled during the encryption process, making it impossible for the firewall, proxy server or NAT to deliver the data to the requesting user. In contrast, the present invention accurately separates the payload and non-payload parts, encrypting only the payload part so that the data appears unchanged to the firewall, proxy server or NAT that requires only the non-payload part to affect delivery to the user requesting the data stream.

'175 patent, 8:58–9:3.

Widevine finds fault with Verimatrix's proposal because it implies a physical separation of data that the claims do not require. Verimatrix, on the other hand, argues that substituting Widevine's construction for "parsing", Verimatrix argues, yields a nonsensical result: "[analyzing data to differentiate between different portions of data] the received packet data into portions." *See* '175 patent, Claim 19. The Court agrees with both parties; neither proposal is appropriate. The parties have already agreed to what a parser does. The Court adopts a construction that captures the parties' agreement, as well as substitutes into the claims cleanly. "Parsing" means "differentiating."

C. "data type"

Term	**Widevine Construction**	**Verimatrix Construction**
Data type	Data that corresponds to a particular type or format of data.	format by which the content in the payload portion is organized.

There is very little intrinsic evidence to guide the Court's construction of "data type." The specification uses "data type" in only a few places, but each time equating "data type" with a multimedia or streaming format, like Windows Media format.[1] The abstract does not use "data type," but uses the word "media format" in a manner that is consistent with the claims' use of "data type."[2]

Widevine urges the Court to reject a definition of data type that means "format" or its equivalent. Widevine points to the prosecution history, in which the applicant thrice amended the language immediately surrounding "data type." The language in '175 patent, claim 1 changed from the following text in June 2004:

> an encrypter configured to determine if the first portion of the data is to be encrypted based on a format of the first portion of the data, and if it is to be encrypted, to encrypt the first portion of the data

to this in March 2005:

> an encrypter configured to determine if the first portion of the data is to be encrypted ~~based on a format of~~ by inspecting the first portion of the data, the inspection being independent of a packet header, and if it is to be encrypted, to encrypt the first portion of the data

and finally, in July 2005, became:

> an encrypter configured to determine if the ~~first~~ payload portion of the data is to be encrypted by ~~inspecting~~ examining the ~~first~~ payload portion of the data to recognize a predefined data type, ~~the inspection being independent of a packet header,~~ and if it is to be encrypted, to encrypt the ~~first~~ payload portion of the data

According to Widevine, these amendments are inconsistent with defining "data type" to be "format." The Court disagrees that the prosecution history indicates such a rejection of "format." The amendments increase the specificity in the claim language regarding how the invention

[1] "[I]f the encryption unit does not see a data type that it specifically recognizes, then it ignores it, but if the encryption unit sees a data type that it does recognize (e.g. Multimedia content), then it selectively encrypts only the recognized portion of the data stream." '175 patent, 5:27–32. "[T]he EB system provides parsing and encryption for a variety of data types and streams including but not limited to Windows Media format and RTP/RTSP using TCP, TCP/UDP or http delivery." '175 patent, 7:17–20.

[2] "The apparatus is platform independent in terms of media format and data protocol. The encryption unit encrypts data transparently to the client based on the media format." '175, Abstract. The claim language describes this selective encryption based on "data type" rather than "media format."

performs selective encryption. The language in the July 2005 amendment, "encrypted by examining the payload portion of the data to recognize a predefined data type," is a more explicit way of saying that which appears in the June 2004 amendment, "encrypted based on a format of the first portion of the data."

Furthermore, Widevine's proposal incorrectly equates "data type" with data. A "data type" is not data. Rather, it is the manner in which data is stored. The Court construes "data type" to be "format by which the content in the payload portion is organized."

D. "decryption shim" or "shim"

Term	Widevine Construction	Verimatrix Construction
Decryption shim **shim**	A software component that is downloaded to or pre-installed on the client machine and used to decrypt incoming data stream from the encryption bridge on its way to the media player software.	transparent software that is downloaded to or pre-installed on the client machine and used to decrypt incoming data stream from the encryption bridge on its way to the media player software.

The parties dispute whether the construction for "decryption shim" should include the word "transparent." The language the parties agree upon comes from the specification, which Verimatrix contends is an express definition:

> The invention further provides a client system, also referred to as a decryption shim or simply a shim, ***which is a piece of transparent software that is downloaded to or pre-installed on the client machine*** (e.g. personal computer, network appliance or other network capable device) ***and used to decrypt incoming data streams from the EB on its way to the media player software.***

'175 patent, 9:50–56. The issue is whether "transparent" would be an unnecessary limitation imported from the specification into the claims.

Widevine argues, under the doctrine of claim differentiation, that including "transparent" in the definition of "shim" would make that word meaningless in Claim 57, which recites "the shim being configured so that the negotiating and exchanging of the key thereby and the decrypting of the data thereby is transparent to the user." *See* '175 patent, Claim 57. Apparatus Claim 81, on the other hand, only uses the word "shim" in the preamble, but does not use the word "transparent" in the body. According to Widevine, Claim 81 is implicitly transparent and the limitations teach how the shim operates transparently. However, "claim differentiation is not a 'hard and fast rule of construction,' and cannot be relied upon to 'broaden claims beyond their correct scope.'" *Wenger Mfg., Inc. v. Coating Mach. Sys., Inc.*, 239 F.3d 1225, 1233 (Fed. Cir. 2001). The intrinsic evidence convinces the Court that the inventor intended the "shim" to be transparent, notwithstanding the doctrine of claim differentiation. *See Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1370 (Fed.Cir.2007) ("the written description and prosecution history overcome any presumption arising from the doctrine of claim differentiation").

The Court does, however, need to clarify the definition provided by the patentee in the specification. While the definition of "shim" is express, a mere two paragraphs later in the specification, the patentee explains some exceptions to the software's transparency:

> The installation of the decryption shim is transparent to the user and does not cause a reboot, restart of the user's browser or require interaction. Some exception such as the Mac OS^{TM} and Windos N^{TM} or Windows 2000^{TM} in secure environments or Linux or Unix based client machines because transparent installation requires administrative user privileges on the client machine and the ability of the client machine to receive programs via the Active-X^{TM} mechanism.

'175 patent, 10:27-36. The specification recognizes a distinction between *installation* and *operation* and indicates that the shim will operate transparently, but may not install transparently. To account for this exception, yet remain consistent with the patentee's express definition, the Court construes "shim" and "decryption shim" to mean "software that is downloaded to or pre-installed on the client machine and used to decrypt transparently incoming data stream from the encryption bridge on its way to the media player software."

E. “examining the payload portion of the packet data” and its variants

Term	Widevine Construction	Verimatrix Construction
Examining the payload portion of the packet data . . .	Plain and ordinary meaning based on construction of “packet” and “payload portion.” Insertion of “only” is extraneous and contrary to the plain language of the claims.	examining only the payload portion of the packet data . . .

The parties dispute whether the invention examines the payload portion of the packet to the exclusion of the non-payload portion when it decides to encrypt a packet. Widevine argues that the claims allow the invention to encrypt based upon an examination of non-payload information as well. Verimatrix argues that the patentee, overcoming a prior art rejection, disavowed that claim scope during prosecution. *See* Verimatrix Brief at 12–13.

The Court does not see any disavowal of claim scope. The statements the patentee made to the patent examiner are not inconsistent with examining both the payload and non-payload portions of a packet because the references that the patentee overcame did not examine the payload at all. The distinction over the prior art is that the invention *does* examine the payload, not that it examines the payload *exclusively*. The Court construes the phrase “examining the payload portion of the packet data,” and its variants, to be “examining at least the payload portion of the packet data.”

F. “to encrypt the payload portion of the packet data” and its variants

Term	Widevine Construction	Verimatrix Construction
to encrypt the payload portion of the packet data . . .	Plain and ordinary meaning based on construction of “encrypt” and “payload portion.” Insertion of “only” is extraneous and contrary to the plain language of the claim.	to encrypt only the examined payload portion of the packet data . . .

The parties dispute how much of a packet the invention encrypts. Verimatrix seeks to add “only the examined” to every limitation that recites encryption of the payload portion. Under Widevine’s proposal, on the other hand, the encryption bridge is capable of encrypting the entire packet.

The common specification of the ‘175 and ‘831 patents criticizes the prior art for encrypting an entire packet and explains the benefits of the invention’s ability to encrypt only the payload portion of the packet:

> With current encryption solutions that encrypt data less discriminately, the data is unable to be delivered across unmodified firewalls, proxy servers and NATs. For instance, when a user requests data from a streaming server, that data stream is organized into packets that have specific data for identifying the target use. Without accurately parsing the data into payload and non-payload parts, the user specific data is readily damaged or scrambled during the encryption process, making it impossible for the firewall, proxy server or NAT to deliver the data to the requesting user. In contrast, ***the present invention accurately separates the payload and non-payload parts, encrypting only the payload part.***

‘175 patent, l8:65–67. Similar language appears in the abstract, as well: “encrypting only the first portion of the data . . . wherein the second portion of the data is not encrypted.” ‘175 patent, Abstract. As a solution to the problem created by encrypting an entire packet, the invention use “selective encryption” to leave the non-payload portion of a packet intact. *See* ‘175 patent, 5:18–24. Yet another excerpt from the specification unambiguously describes the invention as encrypting only the payload portion of a packet:

> [T]he invention provides a software bridge that examines network data passing through, parses the network data and only encrypts the relevant payload part, leaving the non-payload part that may include data such as routing, size and other header data surrounding the payload part entirely untouched.

‘175 patent, 8:18–25.

This is one of those cases where the “specification makes clear that the invention does not include a particular feature.” *SciMed Life Sys. V. Advanced Cardiovascular Sys.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001). Here, the invention does not include the feature of encrypting anything more than the payload portion of a packet and permits the Court to interpret the claim term more narrowly than it otherwise would. *See Honeywell Int'l, Inc. v. ITT Indus., Inc.,* 452 F.3d 1312, 1319-20 (Fed. Cir. 2006). The Court construes the phrase "to encrypt the payload portion of the packet," and its variants, to mean "to encrypt only the payload portion of the packet."

G. "as determined by an examination of the payload portion of the packet data to recognize a predefined data type"

Term	Widevine Construction	Verimatrix Construction
as determined by an examination of the payload portion of the packet data to recognize a predefined data type	As determined by another device prior to encryption through an examination of the unencrypted payload portion to recognize a predefined data type.	as determined at the client by an examination of the payload portion of the packet data to recognize a predefined data type, decrypting the payload portion of the packet data

The parties argue where the payload is examined, as recited in Claim 37. Widevine argues that the payload is examined "by another device prior to encryption." Verimatrix argues that the payload is examined at the client. Claim 37, with the disputed language emphasized, is below:

> A method for streaming data at a client, the data including payload and non-payload portions which differ from each other in at least one characteristic, the streaming data is included in a plurality of packets having been sent over a network to the client from an encryption source, the method comprising:
>
> receiving the packet data sent over the network;
>
> parsing the packet data into portions including the payload and non-payload portions;
>
> if the payload portion of the packet data is encrypted based on a format of the payload portion of the packet data, **as determined by an examination of the payload portion of the packet data to recognize a predefined data type**, decrypting the payload portion of the packet data; and
>
> passing the decrypted payload portion of the packet data to a higher level of operations for play in the client.

'175 patent, Claim 37.

Widevine argues that the "as determined by" clause explains how the packet is encrypted. Verimatrix argues that the entire claim occurs at a client, as recited in the preamble, and the "as determined by" language, therefore, explains how the client determines whether the payload portion of a received packet is encrypted. Verimatrix also argues that Widevine's proposal introduces imbiguity with "another device," and improperly reads a temporal limitation into the claim with "before encryption."

The intrinsic evidence overwhelmingly points to the conclusions that the format in the phrase "encrypted based on a format" is determined by examining the payload portion, and the encryption bridge—not the client—encrypts a payload only if it recognizes the data type in the payload portion. Verimatrix has not relied on any support in the intrinsic evidence to show that a decryption shim examines a payload to recognize a predefined data type. "Examination of the payload portion of the packet data to recognize a predefined data type," as recited in the claim, occurs at the encryption bridge. The parties have already agreed upon a definition for "encryption bridge." The Court construes "as determined by an examination of the payload portion of the packet data to recognize a predefined data type" to mean, "as determined at the encryption bridge through an examination of the unencrypted payload portion to recognize a predefined data type."

H. "wherein the format is determined by an examination of that payload portion of the packet data to recognize a predefined data type"

Term	Widevine Construction	Verimatrix Construction
wherein the format is determined by an examination of that payload portion of the packet data to recognize a predefined data type	Wherein the format was determined by another device prior to encryption by examining that payload portion of the packet data to recognize a predefined data type.	wherein the format is determined at the client by an examination of that payload portion of the packet data to recognize a predefined data type

As with Claim 37, the parties dispute where and when the determining step occurs. Widevine argues that the payload portion is examined during the encryption process, "at another device." Verimatrix argues that the disputed language modifies data receiver and the examination occurs at the client. The language of Claim 81 is below.

> A shim deployed on a client, the shim comprising:

> a data receiver configured to receive partially encrypted packet data transmitted to the client, wherein another device parsed the packet data into a payload portion and a non-payload portion and determined the payload portion of the packet data to be encrypted based on a format of the payload portion of the packet data, **wherein the format is determined by an examination of that payload portion of the packet data to recognize a predefined data type**;
>
> a parser configured to parse the partially encrypted packet data to select the payload portion of the packet data to be decrypted;
>
> a decrypter configured to decrypt the payload portion of the packet data selected for decrypting by the parser;
>
> and a data transmitter configured to send the decrypted packet data to a higher level operation resident on the client.

‘175 patent, Claim 81.

The term “format” in the disputed clause refers back to the previous clause, “encrypted based on a format of the payload portion of the packet data,” which describes the function performed by “another device.” The “shim deployed on a client” comprises a data receiver “configured to receive partially encrypted packet data,” which means that the client does not perform the encryption, but receives data that has already been encrypted. That is, by the plain language of the claims, the packet is encrypted at “another device.” Therefore, it is “another device,” and not the client, examines the packet to determine the format. The construction for the disputed phrase is, “wherein the format was determined by another device by examining that payload portion of the packet data to recognize a predefined data type.”

I. "first device" and "second device"

Term	Widevine Construction	Verimatrix Construction
a first device that is operative to perform actions, including: receiving a packet; examining a payload portion of the packet for a predefined data type, and if the payload portion includes the predefined data type, selectively encrypting the payload portion; and communicating the selectively encrypted payload portions over the network in a packet.	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "device," "first device" and other terms.	35 U.S.C. § 112(6) element: Function: A first device for performing actions, including: receiving a packet; examining a payload portion of the packet for a predefined data type, and if the payload portion includes the predefined data type, selectively encrypting the payload portion; and communicating the selectively encrypted payload portions over the network in a packet. Structure: Encryption bridge implemented on a computer system which is located between the multiple servers and clients. ('831 Patent, 6:4-35, 6:41:45; 7:51-60; 7:25-31.) The specification and claims do not disclose any algorithm other than RSA, DES-X, or Blowfish for encryption.
a second device that is operative to perform actions, including: receiving the communicated packet, parsing the received packet into the payload and the non-payload portion, and decrypting the selectively encrypted payload portion **and** **negotiate and exchange a key for use in at least one of encrypting or decrypting the selectively encrypted payload portion with another device**	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "device," "second device" and other terms.	35 U.S.C. § 112(6) element: Function: A second device for performing actions, including: receiving the communicated packet, parsing the received packet into the payload and the non-payload portion, and decrypting the selectively encrypted payload portion and negotiating and exchanging a key for use in at least one of encrypting or decrypting the selectively encrypted payload portion with another device Structure: Decryption shim which is deployed to the client by the encryption bridge, is implemented via pluggable/exchangeable architecture, receives, parses, and decrypts the payload portion of the packet. The decryption shim negotiates and exchanges a key. ('831 Patent, 7:3-5; 9:58-10:56; Fig. 3- 330, 340, 360; Fig 5 - 510.) The specification and claims do not disclose any algorithm.

"First device" and "second device" appear in the '831 patent, Claims 16 and 17. The parties dispute whether these terms require construction. Widevine argues that these terms need no construction and should be given their plain and ordinary meaning: networked computing devices. Verimatrix argues that the claims are means-plus-function claims because "device" is a generic term. Claim 16 in its entirety follows:

> A system for managing data securely over a network, comprising:
>
> a first device that is operative to perform actions, including:
>
> > receiving a packet;
> >
> > examining a payload portion of the packet for a predefined data type, and if the payload portion includes the predefined data type, selectively encrypting the payload portion and;
> >
> > communicating the selectively encrypted portions over the network in a packet; and
>
> a second device that is operative to perform actions, including:
>
> > receiving the communicated packet,
> >
> > parsing the received packet into the payload and the non-payload portion, and
> >
> > decrypting the selectively encrypted payload portion.

Verimatrix points to a number of extrinsic references showing that "device" is used indiscriminately to refer to any type of electronic thing and argues that the surrounding claim language does not identify any structure. The Court agrees. The claim provides no structural context and describes each "device" by the functions that it performs, which means that "one of skill in the art would have no recourse but to turn to the [patent's] specification to derive a structural connotation." *Welker Bearing Co. v. PHD, Inc.*, 550 F.3d 1090, 1096 (Fed. Cir. 2008). Therefore, the Court is of the opinion that "first device" and "second device" are means-plus-function limitations and are therefore governed by 35 U.S.C. § 112(6).

The Court must now identify, if any, "the corresponding structure, material, or acts described in the specification and equivalents thereof." 35 U.S.C. § 112(6). "For computer-implemented means-plus-function claims where the disclosed structure is a computer programmed to implement an algorithm, 'the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm.'" *Finisar Corp. v. DirecTV Group, Inc.*, 523 F.3d 1323, 1340 (quoting *WMS Gaming, Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999)). Specifically, the corresponding structure to be found in the specification is the algorithm that performs the claimed function. *Harris Corp. v. Ericsson, Inc.*, 417 F.3d 1241, 1253 (Fed. Cir. 2005). The algorithm must provide sufficient structure to allow a person of ordinary skill in the art to program the computer to perform the functions. *Id.* at 1340–41. It is "important to determine whether one of skill in the art would understand the specification itself to disclose the structure, not simply whether that person would be capable of implementing the structure." *See Atmel Corp. v. Info. Storage Devices, Inc.*, 198 F.3d 1374, 1382 (Fed.Cir.1999). The Federal Circuit "does not impose a lofty standard in its indefiniteness cases." *Finisar*, 523 F.3d at 1341 (citing *Med. Instrumentation & Diagnostics Corp. v. Elekta AB*, 344 F.3d 1205, 1214 (Fed. Cir. 2003)).

Notwithstanding the relatively low standard, this Court finds that the '831 patent, Claim 16 lacks supporting structure in the specification for each of the claimed functions. The Court agrees with Verimatrix that the "first device" is the "encryption bridge implemented on a computer system which is located between the multiple servers and clients. ('831 Patent, 6:4-35, 6:41:45; 7:51-60; 7:25-31.)" and that the "second device" is the "decryption shim which is deployed to the client by the encryption bridge, is implemented via pluggable/exchangeable architecture, receives, parses, and decrypts the payload portion of the packet. The decryption shim negotiates and exchanges a key. ('831 Patent, 7:3-5; 9:58-10:56; Fig. 3- 330, 340, 360; Fig 5 - 510.)." Defendant's Brief, Ex. 1. However, the Court is unable to find a sufficiently detailed algorithm within the specification to provide the necessary structure for all of the functions claimed in Claim 16. The only algorithms identified by either party are the RSA, DES-X, or Blowfish algorithms for encryption that are discussed in the specification. '175 patent, 8:6–17. These algorithms provide supporting structure for the function of "selectively encrypting the payload portion." Because there are no other algorithms in the specification, the remaining functions in Claims 16 and 17 lack the necessary supporting structure.

In addition to a dearth of briefing on the topic of whether the specification discloses an algorithm for the functions claimed, lacking before the Court is the expert testimony upon which it ordinarily relies when construing means-plus-function terms. While the specification does recite the functions in Claim 16, the specification fails to explain sufficiently how one skilled in the art might perform those functions. *See* '831 Patent, 8:27–58; 9:58–10:50; *Finisar*, 523 F.3d at 1340 (failing to find an algorithm where the specification "provides nothing more than a restatement of the function, as recited in the claim") (internal quotations omitted). Independent claim 16 and dependent claim 17 of the '831 Patent are invalid for indefiniteness.

J. "component"

Term	Widevine Construction	Verimatrix Construction
[downloading onto the other network device,] a component that is configured to enable the other network device to decrypt the selectively encrypted payload portion of the other packet	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "component" and other terms. Component = "a downloadable software component"	35 U.S.C. § 112(6) element: Function: A component for enabling the other network device to decrypt the selectively encrypted payload portion of the other packet. Structure: Decryption shim which is deployed to the client by the encryption bridge, is implemented via pluggable/exchangeable architecture, parses and decrypts the payload portion of the packet, and uninstalls itself after use. ('831 Patent, 9:58-64; 10:6; Fig.3 – 360.) The specification and claims do not disclose any algorithm.
[enabling downloading and installing of] a component…for use in decrypting the selectively encrypted payload portions of the streamed packets	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "component" and other terms. Component = "a downloadable software component"	35 U.S.C. § 112(6) element: Function: A component for decrypting the selectively encrypted payload portions of the streamed packets. Structure: Decryption shim which is deployed to the client by the encryption bridge, is implemented via pluggable/exchangeable architecture, parses and decrypts the payload portion of the packet, and uninstalls itself after use. ('831 Patent, 9:58-64; 10:6; Fig.3 – 360.) The specification and claims do not disclose any algorithm.

The parties dispute whether "component" is a means-plus-function term. The surrounding claim language indicates that the component is software that is downloaded onto a computing device.

Verimatrix argues that "component" is a generic term and the claims in which it is found are subject to 35 U.S.C. § 112(6). Verimatrix further argues that the word "component" requires context to have sufficient structure and the claims do not provide the needed context. Widevine argues that surrounding claim language provides sufficient structure to "component" and that it should be construed as "a downloadable software component." The specification's description of a decryption shim is consistent with the claims' use of the term "component." Unlike "device," "component" does not refer to a general purpose computer that is programmed to perform specified functions. "Component" refers to software that is an element of the "computer-readable storage medium" of Claim 9 or an element of the "encryption bridge" of Claim 1. The Court finds that the claim provides sufficient structure to "component," as recited in the '831 Patent, Claims 3, 4, 11, and 12, and is therefore not governed by 35 U.S.C. § 112(6). "Component" means "a downloadable software component."

K. "analyzer"

Term	**Widevine Construction**	**Verimatrix Construction**
Analyzer	Software in the shim that monitors the properties or characteristics of a computing device.	Verimatrix contends that this element is a 35 USC § 112(6) element.

Term	Widevine Construction	Verimatrix Construction
analyzer configured to analyze behavior of the client to detect known media piracy techniques and to terminate the streaming session if a known media piracy technique is detected	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "analyzer" and other terms.	35 U.S.C. § 112(6) element: Function: An analyzer analyzes behavior of the client to detect known media piracy techniques and to terminate the streaming session if a known media piracy technique is detected. Structure: Decryption shim which is deployed to the client by the encryption bridge and is implemented via pluggable/exchangeable architecture and detects known media piracy techniques and end streaming sessions if detected. ('175 patent, 10:2-4; Fig. 3 384.) The specification and claims do not disclose any algorithm.
analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the streaming session if specific behavior is detected	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "analyzer" and other terms.	35 U.S.C. § 112(6) element: Function: An analyzer analyzes a behavior of the client to detect suspicious client behavior and to terminate the streaming session if specific behavior is detected. Structure: (See '175: claim 85.) Decryption shim which is deployed to the client by the encryption bridge and is implemented via pluggable/exchangeable architecture and detects suspicious client behavior and end streaming sessions if detected. ('175 patent, 10:2-4; Fig. 3 384.) The specification and claims do not disclose any algorithm.
analyzer configured to analyze behavior of the client to detect known media piracy techniques and to terminate operation of at least the decrypter when a media piracy technique is detected	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "analyzer" and other terms.	35 U.S.C. § 112(6) element: Function: An analyzer analyzes the behavior of the client to detect known media piracy techniques and to terminate operation of at least the decrypter when a media piracy technique is detected. Structure: (See '175: claim 85.) Decryption shim which is deployed to the client by the encryption bridge and is implemented via pluggable/exchangeable architecture and detects known media piracy techniques and end streaming sessions if detected. ('175 patent, 10:2-4; Fig. 3 384.) The specification and claims do not disclose any algorithm.

Term	Widevine Construction	Verimatrix Construction
analyzer configured to analyze a behavior of the client to detect suspicious client behavior and to terminate the operation of at least the decrypter if suspicious behavior is detected	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of “analyzer” and other terms.	35 U.S.C. § 112(6) element: Function: An analyzer analyzes a behavior of the client to detect suspicious client behavior and to terminate the operation of at least the decrypter if suspicious behavior is detected. Structure: (See ‘175: claim 85.) Decryption shim which is deployed to the client by the encryption bridge and is implemented via pluggable/exchangeable architecture and detects suspicious client behavior and end streaming sessions if detected. (‘175 patent, 10:2-4; Fig. 3 384.) The specification and claims do not disclose any algorithm.

The parties dispute whether “analyzer” is governed by 35 U.S.C. § 112(6). Widevine argues that “analyzer” is a colloquial term that refers to a physical device that analyzes data and should be construed as “software in the shim that monitors the properties or characteristics of a computing device.” Verimatrix argues that “analyzer” is a generic term that does not connote a particular structure, the remainder of the claim does not provide the necessary structure, and is therefore equivalent to “means for analyzing.”

“Shim,” of which “analyzer” is an element, has an agreed construction: “software that is downloaded to or pre-installed on the client machine and used to decrypt transparently incoming data stream from the encryption bridge on its way to the media player software.” The agreed construction provides the necessary structure for “analyzer.” “Analyzer” is therefore not governed by 35 U.S.C. § 112(6). “Analyzer” means “software in the shim that analyzes monitors the properties or characteristics of a computing device.”

L. “data combiner”

Term	Widevine Construction	Verimatrix Construction
Data combiner	Software on a computing device that combines different portions of input data into a single output.	Verimatrix contends that this element is a 35 USC § 112(6) element, see discussion below at entry nos. 49, 50, 51

Term	Widevine Construction	Verimatrix Construction
data combiner configured to combine the encrypted payload portion of the packet data with the non-payload portion of the packet data, wherein the non-payload portion of the packet data includes more than routing information	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "data combiner" and other terms.	35 U.S.C. § 112(6) element: Function: The data combiner combines the encrypted payload portion of the packet data with the non-payload portion of the packet data, wherein the non-payload portion of the packet data includes more than routing information. Structure: The specification does not disclose a data combiner. The specification and claims do not disclose any algorithm.
data combiner configured to combine the encrypted payload portion with at least one unencrypted non-payload data portion	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "data combiner" and other terms.	35 U.S.C. § 112(6) element: Function: A data combiner combines the encrypted payload portion with at least one unencrypted non-payload data portion. Structure: The specification does not disclose a data combiner. The specification and claims do not disclose any algorithm.
data combiner configured to combine the encrypted payload portion of the packet data with an unencrypted portion of packet data for transmission over the network	This is not a means-plus-function limitation. There is no need to construe this limitation further in light of constructions of "data combiner" and other terms.	35 U.S.C. § 112(6) element: Function: A data combiner combines the encrypted payload portion of the packet data with an unencrypted portion of packet data for transmission over the network. Structure: The specification does not disclose a data combiner. The specification and claims do not disclose any algorithm.

The parties dispute whether "data combiner" is governed by 35 U.S.C. § 112(6). Widevine proposes that "data combiner" should be construed as "software on a computing device that combines different portions of input data into a single output," arguing that the specification implicitly supports its proposed construction. Verimatrix argues that "data combiner" does not connote any particular structure and the surrounding claim language does not provide the needed structure. According to Verimatrix, "data combiner" is a coined term commonly used in the art that refers to a category of structures that combine data. In Verimatrix's view, sufficient context is necessary to identify which structure of the category is intended. Verimatrix also argues that the prosecution history shows that the claim limitations were initially drafted using means-plus-function language.

The Court finds that the surrounding claim language provides the necessary structure. The parties agreed that both parser and encrypter are "software on a computing device" and, as both are elements of the apparatus of Claims 1, 58, and 70, so too is "data combiner." In that context, "data combiner" is "software on a computing device that combines different portions of input data into a single output."

M. "sending the packet data into the payload and non-payload portions"

Term	'175 Claims	'831 Claims	Widevine Construction	Verimatrix Construction
Sending the packet data into the payload and non-payload portions	35		Sending the packet data including the payload and non-payload portions	indefinite

Verimatrix argues that '175 patent, Claim 35 is indefinite because "sending the packet data into the payload and non-payload portions" has no discernible meaning and cannot be given meaning during claim construction. Widevine proposes a construction that gives the term a meaning, but does not support its construction with any briefing. The disputed Claim 35 recites: "The method of claim 34, further comprising continuing parsing, encrypting and sending the packet data ***into the payload and non-payload portions*** if it is determined that the client is not compromised."

A claim term is "insolubly ambiguous" when "[t]he intrinsic record does not compel a narrowing of the claim language to any one of the possible definitions." *Honeywell Int'l, Inc. v. Int'l Trade Comm'n,* 341 F.3d 1332, 1338–39 (Fed. Cir. 2003). The emphasized portion of the claim is subject to two possible interpretations. The word "into" could be replaced with "including," which yields the following language: "sending the packet data including the payload and non payload portions." This is consistent with the '175 patent, Claim 19, which recites "sending the received packet data including the encrypted payload portion and non-payload portion." Alternatively, Claim 35 could be corrected to read, "parsing into the payload and non-payload portions," which is also consistent with Claim 19. Because both corrections to the typographical error are reasonable, the claim is ambiguous and therefore invalid for indefiniteness.

VI. Conclusion

The court adopts the constructions set forth in this opinion for the disputed terms of the '175 and '831 patents. The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the court.

SIGNED this 4th day of November, 2009.

T. John Ward

T. JOHN WARD
UNITED STATES DISTRICT JUDGE